

QRadar Security Information and Event Management Appliances
Control Number: 12-055

JUSTIFICATION AND APPROVAL
FOR EXCEPTION TO FAIR OPPORTUNITY

1. Contracting Activity: Department of Veterans Affairs (VA)
Office of Acquisition Operations
Technology Acquisition Center
1701 Directors Blvd, Ste 600
Austin, TX 78744
2. Description of Action: This proposed action is for a firm-fixed-price (FFP) delivery order (DO) issued under the National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) IV Government-Wide Acquisition Contract (GWAC) to obtain five QRadars Security Information and Event Management (SIEM) appliances and associated perpetual license upgrades. The 5 QRadars SIEMs include warranty/maintenance. The QRadars SIEM appliances and software license upgrades will be delivered within 30 days after award. The warranty/maintenance will be for a 12 month period commencing upon VA's acceptance of the QRadars SIEM appliances and licenses. The total estimated value of the proposed action is \$676,377.23.
3. Description of Supplies or Services: VA's Continuous Readiness Information Security Program (CRISP) requires system security monitoring of all system logs and network connectivity to provide event and log correlation, event alerting and information security threat intelligence, and reporting, for data center systems and networks. Using combined event processors and flow collectors, QFlow Collectors, Event Processors, Flow Processors, and QFlow Collectors, collectively referred to as QRadars brand name SIEM hardware appliances, will meet all of these requirements. The appliances include standard software and licenses; however, license upgrades are needed to obtain improved functionality. Finally, VA requires warranty/maintenance to begin once the five new QRadars SIEM appliances and software license upgrades are accepted; the required warranty/maintenance includes 24/7 telephone and email support, software updates, patches, defect support and parts replacement for one-year.
4. Statutory Authority: The statutory authority permitting an exception to fair opportunity is Section 41 U.S.C. 4106(c) as implemented by FAR Subpart 16.505(b)(2)(i)(B), entitled, "Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized."
5. Rationale Supporting Use of Authority Cited: Based on market research, as described in paragraph 8 of this document, limited competition is available among authorized resellers for these brand name items. This is a brand name justification in support of FAR 11.105, Items Peculiar to One Manufacturer. No other appliances are interoperable and compatible with the current production QRadars SIEM architecture.

QRadar Security Information and Event Management Appliances
Control Number: 12-055

The requirement for VA CRISP compliance applies to the Corporate Data Center Operations (CDCO) SIEM architecture in use at each of the Information Technology Centers (ITCs). Quantico Information Technology Center (QITC) and Capitol Regional Data Center (CRDC) are the two remaining centers of five requiring SIEM appliances. The new QRadars SIEM appliances and software license upgrades must match the existing CDCO QRadars SIEM architecture in use at the other CDCO data centers. The reason is because Austin Information Technology Center (AITC) Security Operations Center (SOC) centrally manages IT security operations of all five CDCO data centers, and they must use the same SIEM architecture from the same centralized SIEM console. No other appliances will be capable of working with the current architecture, connectivity, licensing, and management within CDCO's production QRadars SIEM architecture and configuration.

VA has a significant investment in its security operations architecture. If any other brand name appliances were to be introduced, VA would require extensive redevelopment efforts to expand the current CDCO Security SIEM architecture. Other SIEM devices and solutions will not communicate the same way as the QRadars architecture, which IBM QRadars owns and developed. The way each event collector and processor operates and transmits metadata to the console is not a function that is interchangeable between other SIEM architectures except for QRadars. The estimated cost for a SIEM retool would be over \$3 million for materials and equipment, \$100,000 for VA staff training to learn how to use the new application.

Additionally, only QRadars SIEM appliances and QRadars software license upgrades can meet the following functional requirements needed:

- Browser based monitoring console that is configurable and distributable by user roles
- Agent-less deployment as well as have an auto discovery for network assets and process for network assets, compress data stored as well as transmit metadata between the collectors and console, raw data transmits is not expected to introduce new network bandwidth loads, metadata needs to be encrypted between collectors and main console and only transmit the deltas, RAW data access needs to be available on the collectors for deep analysis at any given point from the metadata information without additional steps of RAW data imports
- Ability to collect logs from various systems and formats, including International Business Machines (IBM) zVM and zOS operating systems, VMware virtual network flow not found in syslog events, but found between vSwitches on Host systems hosting virtual machines
- Customizable for new log formats
- Ability to store 6 years of logs, licensing does not need to know hosts/IP's and is device number dependent. The licensing model must be based on events per second or events per minute, volume licensing at the hardware side in increments

QRadar Security Information and Event Management Appliances
Control Number: 12-055

- Malware detection based on behavioral baselines and not signature-dependent allowing for deep analysis and no reliance on operating system maintenance or management

A decision to use another SIEM solution would require the current QRadar devices to be removed from each CDCO ITC, production use stopped, and then a plan to install replacement of SIEM devices for five ITCs. Each center's deployment includes network devices and additional licensing. The existing investment is \$1.5 million for Austin, \$1 million for Philadelphia, which includes the disaster recovery site with duplicate console hardware, and \$800K for the Hines data center. Additionally, CDCO IT security staff would have to spend approximately one year to retrain VA personnel to use the different SIEM architecture while removing the current QRadar to keep current IT security functions going (and not introduce gaps.) Furthermore, VA technical experts estimate it would require approximately 1.5 man-years of effort to replace and retool the current production QRadar SIEM architecture.

Finally, only a reseller of QRadar products can provide the warranty/maintenance required by VA. In order to ensure the aforementioned brand name items remain operational, any source must have extensive knowledge of the brand name items and access to its proprietary technical data in order to provide effective solutions to any maintenance required. Only authorized resellers can meet that requirement.

6. Efforts to Obtain Competition: Government technical experts performed internet searches and reviewed market literature in order to find additional products that can provide similar functionality as the QRadar products and maintenance. None were found that would provide the functionality described in Section 5. In accordance with FAR 5.301 and 16.505(b)(2)(D)(1)(i), this action will be synopsized at award on the Federal Business Opportunities Page and the justification will be made publically available.

7. Actions to Increase competition: In order to remove or overcome barriers to competition in future acquisitions for this requirement, the agency will perform additional market research so that other solutions can be considered.

8. Market Research: The Government's technical experts performed market research between January 2011 through March 2012 by researching other similar solutions (online and through market literature) to learn if other brand items could meet and be compatible with VA's existing architecture (considering connectivity, licensing and management.) The Government's Information Technology (IT) Security technical experts reviewed similar solutions from the following companies: NitroSecurity, eiQnetworks and Sensage. The items did not meet VA's requirements. None of the appliances reviewed will be able to work with current architecture, connectivity, licensing and management within the CDCO's production QRadar SIEM architecture and configuration. Additionally, none of the appliances reviewed met VA's specific functional requirements detailed in paragraph 5. Based on this market research, the Government's technical experts have concluded that only the QRadar brand name

appliance and software will meet AITC SOC's requirements for its central management of IT security operations requirements for its five ITCs.

9. Other Facts: None

10. Technical and Requirements Certification: I certify that the supporting data under my cognizance, which are included in this justification, are accurate and complete to the best of my knowledge and belief.

Benito Urbina

Date:

8-15-2012

Project Manager

Signature:



11. Fair and Reasonable Cost Determination: I hereby determine that the anticipated price to the Government for this contract action will be fair and reasonable. Prices contained in contracts awarded on NASA SEWP IV GWAC have already been determined to be fair and reasonable. As there are multiple vendors on NASA SEWP IV GWAC, additional price competition is anticipated. Finally, the successful quotation will be compared to the independent government cost estimate.

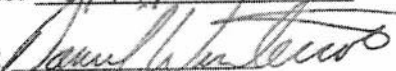
Daniel Winterroth

Date:

8/14/12

Procuring Contracting Officer

Signature:



12. Contracting Officer Certification: I certify that this justification is accurate and complete to the best of my knowledge and belief.

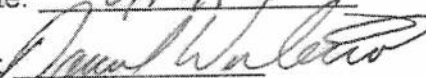
Daniel Winterroth

Date:

8/14/12

Procuring Contracting Officer

Signature:



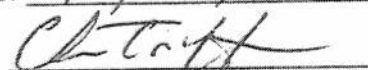
13. Legal Sufficiency Certification: I have reviewed this justification and find it adequate to support an exception to fair opportunity and deem it legally sufficient.

Christopher Tiroff
Legal Counsel

Date:

Aug 15, 2012

Signature:




QRadar Security Information and Event Management Appliances
Control Number: 12-055


Approval

In my role as Contracting Activity Competition Advocate, based on the foregoing justification, I hereby approve a Firm-Fixed-Price Delivery Order issued under the National Aeronautics and Space Administration Solutions for Enterprise-Wide Procurement IV Government-Wide Acquisition Contract to acquire QRadar Security Information and Event Management appliances, associated software license upgrades, and warranty maintenance. This action will be issued as an exception to fair opportunity as specified by FAR 16.505(b)(2)(i)(B), subject to availability of funds, and provided that the property and services herein described have otherwise been authorized for acquisition.

Date: 9/4/12

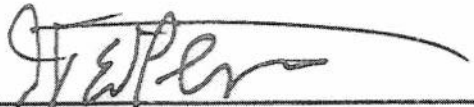
Signature: 
Iris B. Cooper
Head of the Contracting Activity

Justification For An Exception To Fair Opportunity
Coordination Matrix




Ronald J. Bakay
Competition Manager
Technology Acquisition Center (003B2)
Office of Acquisition Operations
Department of Veterans Affairs

Date 8/28/12 Concur/Non-Concur



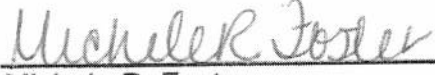
David Peterson
Deputy Director
Acquisition Service - Austin
Technology Acquisition Center (003B2H)
Office of Acquisition Operations
Department of Veteran Affairs

Date 8-17-2012 Concur/Non-Concur



Greg Hamberg
Director
Acquisition Service - Austin
Technology Acquisition Center (003B2H)
Office of Acquisition Operations
Department of Veteran Affairs

Date 8-17-2012 Concur/Non-Concur



Michele R. Foster
Deputy Associate Executive Director
Technology Acquisition Center (003B2A)
Office of Acquisition Operations
Department of Veterans Affairs

Date 8-31-2012 Concur/Non-Concur

Wendy J. McCutcheon
Associate Executive Director
Technology Acquisition Center (001 AL-A3)
Office of Acquisition Operations
Department of Veterans Affairs

Date _____ Concur/Non-Concur